PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-259571
(43)Date of publication of application : 24.09.1999

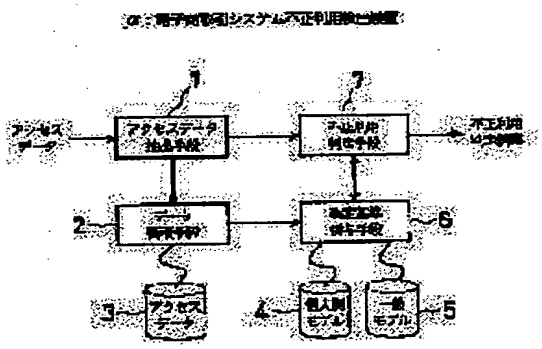
(51)Int.Cl. G06F 17/60
G06F 11/34

(21)Application number : 10-063013
(22)Date of filing : 13.03.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : FUJI HITOSHI
NAKAYAMA RYUJI
IJUIN TADASHI

(54) ELECTRONIC BUSINESS TRANSACTION SYSTEM UNAUTHORIZED UTILIZATION DETECTION METHOD AND DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide electronic business transaction system unauthorized utilization detection method and device capable of detecting the unauthorized utilization of a system by an unauthorized user and an unauthorized client based on the result of monitoring the normal action of a normal user and a normal client.
SOLUTION: This device is provided with a judgement reference supply means 6 for supplying plural data incorporated in an individual model and a general model stored by a data storage means 2 as a judgement standard for judging whether or not the access is by the unauthorized utilization every time new access is executed and an unauthorized utilization judgement means 7 for comparing the plural data incorporated in the individual model and the general model supplied by the judgement standard supply means 6 with new plural data extracted by an access data extraction means 1 accompanying the access and judging whether or not the access is by the unauthorized utilization.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－259571

(43)公開日　平成11年(1999)９月24日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｇ０６Ｆ　17/60		Ｇ０６Ｆ	15/21	３４０Ｚ
11/34			11/34	Ｃ
			15/21	３３０

審査請求　未請求　請求項の数25　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－63013

(22)出願日　平成10年(1998)３月13日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　冨士　仁
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　中山　隆二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　伊集院　正
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

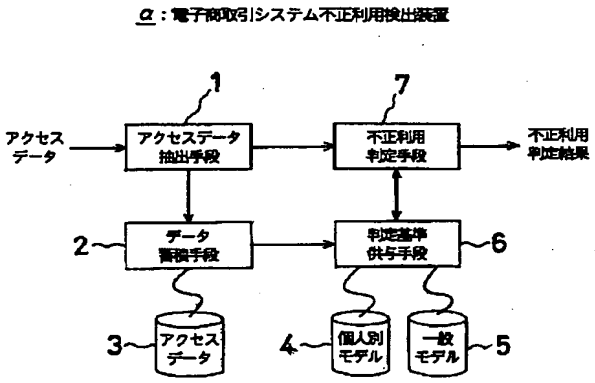
(74)代理人　弁理士　菅　隆彦

(54)【発明の名称】　電子商取引システム不正利用検出方法及び装置

(57)【要約】

【課題】正規ユーザや正規クライアントの通常の行動を監視した結果に基づいて、不正ユーザや不正クライアントによるシステムの不正利用を検出することの可能な電子商取引システム不正利用検出方法及び装置を提供する。

【解決手段】データ蓄積手段２により蓄積された個人別モデル及び一般モデルに組み込まれた複数のデータを、新たなアクセスが実行されるごとに、当該アクセスが不正利用によるものであるか否かを判定するための判定基準として供与する判定基準供与手段６と、この判定基準供与手段６により供与される個人別モデル及び一般モデルに組み込まれた複数のデータと、当該アクセスに伴ってアクセスデータ抽出手段１により抽出される新たな複数のデータとを比較して、当該アクセスが不正利用によるものであるか否かを判定する不正利用判定手段７とを有する。



1

【特許請求の範囲】

【請求項１】電子商取引の不正利用をアクセス毎に常時監視しリアルタイムで検出するに当り、
正規ユーザや正規クライアントのアクセス及びイベント等行動における過去の行動履歴傾向及び習性を参照して判定検出する、
ことを特徴とする電子商取引システム不正検出方法。

【請求項２】前記行動履歴は、
個人別モデルと一般モデルに区分される、
ことを特徴とする請求項１に記載の電子商取引システム不正検出方法。

【請求項３】前記個人別モデルと一般モデルは、
相互に参照優先順位が付与される、
ことを特徴とする請求項１又は２に記載の電子商取引システム不正検出方法。

【請求項４】前記個人別モデルと一般モデルは、
アクセスに伴う単独のイベント記録から直接データが得られるものと、
複数のイベント記録から導き出されるものの両方のデータを利用する、
ことを特徴とする請求項２又は３に記載の電子商取引システム不正検出方法。

【請求項５】前記過去の行動履歴は、
ユーザやクライアントに個人識別子を持たせ、初期画面以降のページの移動時にその情報がプロバイダやサーバに自動的に送信されるよう、当該プロバイダやサーバから前記ユーザやクライアントに送るデータにより当該ユーザやクライアントの機能を制御し、前記個人識別子毎に分けられるデータを当該プロバイダやサーバ内のファイルやメモリ等に蓄積する、
ことを特徴とする請求項１、２、３又は４に記載の電子商取引システム不正検出方法。

【請求項６】前記個人モデルと一般モデルは、
統計処理を行うデータと状態遷移を表すデータの両方を含んでなる、
ことを特徴とする請求項２、３、４又は５に記載の電子商取引システム不正検出方法。

【請求項７】前記状態遷移は、
アクセス行動から不正利用を検出する単独アクセス行動状態遷移と、
過去から現在までの状態遷移の比較によって不正利用を検出する複数アクセス状態遷移とが存在する、
ことを特徴とする請求項６に記載の電子商取引システム不正利用検出方法。

【請求項８】電子商取引を行う任意のクライアント／サーバシステムに対する不正利用を検出するための電子商取引の不正利用を検出するに当り、
クライアントからサーバに対しアクセスが開始された後、前記クライアントから所定のイベントが複数回にわたって発行されるごとに、前記サーバにおいて、前記クライアント及びそのユーザに関する情報並びに当該ユーザによる電子商取引行為に関する情報を複数のデータとして逐次取り込んで、当該複数のデータのそれぞれを、前記ユーザに付与される個人識別子を単位とした個人別モデルに組み込んで蓄積し、
以後、新たにアクセスが実行されるごとに、当該アクセスが開始された後に得られる複数のデータと前記個人別モデルとを比較し、この比較結果に基づいて、当該アクセスが不正利用によるものであるか否かを判定する、
ことを特徴とする電子商取引システム不正利用検出方法。

【請求項９】前記複数のデータの蓄積に際しては、
前記複数のデータのそれぞれを、前記個人別モデルに代え、当該システムを利用する全てのユーザの平均的データを得るための一般モデルに組み込んで行い、
前記アクセスが不正利用によるものであるか否かの判定は、
前記複数のデータと当該一般モデルとを比較した結果に基づいて行う、
ことを特徴とする請求項８に記載の電子商取引システム不正利用検出方法。

【請求項１０】前記複数のデータの蓄積は、
１回のアクセスが終了した時点で得られる全てのデータをその発生順に並べた時系列データによって行う、
ことを特徴とする請求項８又は９に記載の電子商取引システム不正利用検出方法。

【請求項１１】前記時系列データを得るに際しては、
前記所定のイベントが最後に発行されたと予想される時から所定の制限時間が経過した時点で、当該最後の所定のイベントまでを１回のアクセス中に含まれる一連の所定のイベントと見做す、
ことを特徴とする請求項１０に記載の電子商取引システム不正利用検出方法。

【請求項１２】前記アクセスが不正利用によるものであるか否かの判定は、
統計学的手法を用いて行う、
ことを特徴とする請求項８、９、１０又は１１に記載の電子商取引システム不正利用検出方法。

【請求項１３】前記アクセスが不正利用によるものであるか否かの判定は、
１回のアクセス中に複数回にわたって発行される前記所定のイベントに伴う当該システムの状態遷移の不規則性を検出することにより行う、
ことを特徴とする請求項８、９、１０、１１又は１２に記載の電子商取引システム不正利用検出方法。

【請求項１４】前記アクセスが不正利用によるものであるか否かの判定は、
複数のアクセスにおいて取り込まれる同一ユーザのものと予想される前記複数のデータのうち、特定のデータの不規則性を検出することにより行う、

ことを特徴とする請求項８、９、１０、１１又は１２に記載の電子商取引システム不正利用検出方法。

【請求項１５】前記特定のデータは、
前記ユーザによる前記電子商取引に関する情報から成るデータである、
ことを特徴とする請求項１４に記載の電子商取引システム不正利用検出方法。

【請求項１６】前記所定のイベントは、
次の画面の表示を要求するための次画面表示要求イベントである、
ことを特徴とする請求項８、９、１０、１１、１２、１３、１４又は１５に記載の電子商取引システム不正利用検出方法。

【請求項１７】電子商取引を行う任意のクライアント／サーバシステムにおけるサーバに、少なくとも、アクセスの開始と共にクライアントから送信されるアクセスデータを抽出するアクセスデータ抽出手段と、このアクセスデータ抽出手段により抽出された前記アクセスデータを蓄積するデータ蓄積手段とを具備して成る電子商取引システム不正利用検出装置において、
前記アクセスデータ抽出手段は、
前記アクセスデータの抽出に加え、前記アクセスが開始された後、前記クライアントから所定のイベントが複数回にわたって発行されるごとに、前記クライアント及びそのユーザに関する情報並びに当該ユーザによる電子商取引行為に関する情報を包含する複数のデータを抽出する機能を持たせると共に、
前記データ蓄積手段は、
前記アクセスデータの蓄積に加え、前記アクセスデータ抽出手段により抽出された前記複数のデータのそれぞれを、前記ユーザに付与される個人識別子を単位とした個人別モデルに組み込んで蓄積する機能をも持たせ、
その上で、
当該データ蓄積手段により蓄積された前記個人別モデルに組み込まれた複数のデータを、新たなアクセスが実行されるごとに、当該アクセスが不正利用によるものであるか否かを判定するための判定基準として供与する判定基準供与手段と、
この判定基準供与手段により供与される前記個人別モデルに組み込まれた複数のデータと、当該アクセスに伴って前記アクセスデータ抽出手段により抽出される新たな複数のデータとを比較して、当該アクセスが不正利用によるものであるか否かを判定する不正利用判定手段と、
を備える、
ことを特徴とする電子商取引システム不正利用検出装置。

【請求項１８】前記データ蓄積手段は、
前記複数のデータのそれぞれを、前記個人別モデルに代え、当該システムを利用する全てのユーザの平均的データを得るための一般モデルに組み込み、
前記判定基準供与手段は、
当該データ蓄積手段により蓄積された前記一般モデルに組み込まれた複数のデータを、新たなアクセスが実行されるごとに、当該アクセスが不正利用によるものであるか否かを判定するための判定基準として供与し、
前記不正利用判定手段は、
当該判定基準供与手段により供与される前記一般モデルに組み込まれた複数のデータと、当該アクセスに伴って前記アクセスデータ抽出手段により抽出される新たな複数のデータとを比較して、当該アクセスが不正利用によるものであるか否かを判定する、
一連の有機的連係機能をそれぞれ持たせる、
ことを特徴とする請求項１７に記載の電子商取引システム不正利用検出装置。

【請求項１９】前記データ蓄積手段は、
前記複数のデータの蓄積を、１回のアクセスが終了した時点で得られる全てのデータをその発生順に並べた時系列データによって行う機能を有する、
ことを特徴とする請求項１７又は１８に記載の電子商取引システム不正利用検出装置。

【請求項２０】前記データ蓄積手段は、
前記時系列データを得るに際し、前記所定のイベントが最後に発行されたと予想される時から所定の制限時間が経過した時点で、当該最後の所定のイベントまでを１回のアクセス中に含まれる一連の所定のイベントと見做す機能を有する、
ことを特徴とする請求項１８に記載の電子商取引システム不正利用検出装置。

【請求項２１】前記不正利用判定手段は、
前記アクセスが不正利用によるものであるか否かの判定を、統計学的手法を用いて行う演算手段を有する、
ことを特徴とする請求項１７、１８、１９又は２０に記載の電子商取引システム不正利用検出装置。

【請求項２２】前記不正利用判定手段は、
前記アクセスが不正利用によるものであるか否かの判定を、１回のアクセス中に複数回にわたって発行される前記所定のイベントに伴う当該システムの状態遷移の不規則性を検出することにより行う演算手段を有する、
ことを特徴とする請求項１７、１８、１９、２０又は２１に記載の電子商取引システム不正利用検出装置。

【請求項２３】前記不正利用判定手段は、
前記アクセスが不正利用によるものであるか否かの判定を、複数のアクセスにおいて取り込まれる同一ユーザのものと予想される前記複数のデータのうち、特定のデータの不規則性を検出することにより行う演算手段を有する、
ことを特徴とする請求項１７、１８、１９、２０又は２１に記載の電子商取引システム不正利用検出装置。

【請求項２４】前記特定のデータは、
前記ユーザによる前記電子商取引に関する情報から成る

データである、
ことを特徴とする請求項２３に記載の電子商取引システム不正利用検出装置。
【請求項２５】前記所定のイベントは、
次の画面の表示を要求するための次画面表示要求イベントである、
ことを特徴とする請求項１７、１８、１９、２０、２１、２２、２３又は２４に記載の電子商取引システム不正利用検出装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子商取引システム不正利用検出方法及び装置に関し、詳しくは、電子商取引による物品販売などを行う任意のクライアント／サーバシステム（以下、単に「電子商取引システム」という）の利用を許可されていない人物が、正規に許可を受けた人物に成りすまして当該電子商取引システムを不正に利用するのを検出するための電子商取引システム不正利用検出方法、及びその実施に直接使用する電子商取引システム不正利用検出装置に係わる。
【０００２】
【従来の技術】近年、例えば、WWW（World Wide Web）を使ったインターネット上のWWWサイトにおいて、商品カタログを展示するなどして物品の販売を行うバーチャルモール、即ち電子的なショッピングアーケードが設営されている。
【０００３】この種のWWWサイトでは、ユーザ（物品を購入しようとする利用者）がクライアント端末から自身のクレジットカード情報を入力したり、電子マネーを使って決済を行う電子商取引が行われるため、不正利用があった場合には、ショッピングアーケードの運営者に金銭的な被害が及ぶことになる。これを防止するためには、サーバの側で、ユーザが電子商取引システムにアクセスを開始してから決済が行われるまでの短時間のうちに不正利用を検出して、不正ユーザを排除する必要がある。
【０００４】なお、ここにいう「不正利用」とは、ある人物がサーバ管理者から正規の手順を経て入手したＩＤ（Identification）やパスワードなどの個人識別子を、他の人物が正規の手順を経ずに何らかの方法で入手し、それを行使してサーバの機能を利用することや、或いは、システムの欠陥を利用して他の人物に成りすまし、サーバの機能を利用することをいう。また、「不正ユーザ」とは、以上のような不正利用を行う人物をいう。
【０００５】ここで、従来の一般的なコンピュータシステムにおいて採用されている不正利用検出のための手法を挙げれば、
（１）コンピュータシステム内に保存されている各種のログを解析することで、ユーザが許可されていないコマンドの実行などを行ったことを検出し、これを不正利用と見做す手法。
【０００６】（２）コンピュータシステムを構成するソフトウェアの欠陥、設定ミス、不適切な利用などを検査することで、不正利用を行おうとする人物からの攻撃対象になりうる事象を事前にシステム管理者などが調査する手法。
【０００７】（３）コンピュータシステム内に常駐のシステムや、ネットワーク上に設置したネットワークパケットのモニタリングを行うシステムにより、コンピュータシステムに被害を及ぼすことができる特権ユーザ（システム管理の権限を有するユーザ、いわゆるスーパーユーザなどを指し、一般ユーザと区別される）の行動（イベントの要求過程）を監視し、これを予めシステムに登録してある行動パターンと比較して、その行動が不正ユーザのものであるか否かを判断する手法などがある。
【０００８】
【発明が解決しようとする課題】しかしながら、以上に示した不正利用検出のための手法は、あくまで一般的なコンピュータシステムに採用されるものであり、（１）の手法の場合、所要の不正利用の検出を、定期的にログを検査するタイミングでしか行うことができないため、その不正利用の検出にリアルタイム性が求められる電子商取引システムにおいては、何らの効果も期待することができない。
【０００９】（２）の手法の場合、予め存在が確認されている欠陥などを検査することしかできないため、欠陥などが無い状況において行われる不正利用を検出することはできず、上述したのと同様な理由により、この手法の電子商取引システムへの適用には無理あがる。
【００１０】また、（３）の手法の場合、監視する対象である特権ユーザの行動が存在する状況下についてのみしか機能しないため、基本的に、権限が同一のユーザの中から不正ユーザを検出しようとするときには利用できない。特に、問題とされる電子商取引システムにおいては、登録されるユーザの中に特権ユーザは存在せず、ユーザは全て同じ権限を持っており、サーバ内で行えることも同じである。
【００１１】以上のように、何れの手法も、電子商取引システムの不正利用の検出には適用することができない。ただ、以上のことから、電子商取引システムの不正利用の検出に際しては、特権ユーザの行動を監視するのではなく、正規ユーザの通常の行動に基づいてそれを行うのが適切であると考えられ、そのためには、やはり、電子商取引システムへのアクセスに伴ってサーバ内に記録されるログを利用するのが得策である。
【００１２】ここで、上述のサーバ内に記録されるログの種類を考えた場合、例えば、WWWサーバにおいては、クライアントから表示要求の為されたファイル名、要求元クライアントのマシン名、或いは時間などといった、極めて限られた情報のみしかログに記録されない。

【００１３】しかも、WWWサーバの特徴として、同一クライアントからの表示要求であるセッションを、１回ごとに分離して記録することしかできない。このことは、あるユーザが一つの目的のために行った複数のページの表示要求を、サーバ側が、同一のユーザにより為された一連の行動として捕らえられないことを意味している。

【００１４】ここにおいて、本発明の解決すべき主要な目的は次のとおりである。即ち、本発明の第１の目的は、正規ユーザの通常の行動を監視した結果に基づいて、不正ユーザによるシステムの不正利用を検出することの可能な電子商取引システム不正利用検出方法及び装置を提供せんとするものである。

【００１５】本発明の第２の目的は、同一ユーザにより為された一連の行動を把握することの可能な電子商取引システム不正利用検出方法及び装置を提供せんとするものである。

【００１６】本発明の第３の目的は、一般的なユーザの行動様式に基づいてシステムの不正利用を検出することの可能な電子商取引システム不正利用検出方法及び装置を提供せんとするものである。

【００１７】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【００１８】

【課題を解決するための手段】本発明においては、上記課題の解決にあたり、クライアントからサーバに対しアクセスが開始された後に発行される種々の複数のデータを取り込み、これら一旦取り込んでおいた複数のデータのそれぞれと、以後、新たにアクセスが実行されるごとに当該アクセス後に得られる複数のデータとを比較し、この比較結果に基づいて、当該アクセスが不正利用によるものであるか否かを判定する、という手法及び手段を講じる特徴を有する。

【００１９】さらに、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法又は手段を採用することにより、前記目的を達成するよう為される。

【００２０】即ち、本発明方法の第１の特徴は、電子商取引の不正利用をアクセス毎に常時監視しリアルタイムで検出するに当り、正規ユーザや正規クライアントのアクセス及びイベント等行動における過去の行動履歴傾向及び習性を参照して判定検出してなる電子商取引システム不正検出方法の構成採用にある。

【００２１】本発明方法の第２の特徴は、上記本発明方法の第１の特徴における前記行動履歴が、個人別モデルと一般モデルに区分されてなる電子商取引システム不正検出方法の構成採用にある。

【００２２】本発明方法の第３の特徴は、上記本発明方法の第１又は第２の特徴における前記個人別モデルと一般モデルが、相互に参照優先順位が付与されてなる電子商取引システム不正検出方法の構成採用にある。

【００２３】本発明方法の第４の特徴は、上記本発明方法の第２又は第３の特徴における前記個人別モデルと一般モデルが、アクセスに伴う単独のイベント記録から直接データが得られるものと、複数のイベント記録から導き出されるものの両方のデータを利用してなる電子商取引システム不正検出方法の構成採用にある。

【００２４】本発明方法の第５の特徴は、上記本発明方法の第１、第２、第３又は第４の特徴における前記過去の行動履歴が、ユーザやクライアントに個人識別子を持たせ、初期画面以降のページの移動時にその情報がプロバイダやサーバに自動的に送信されるよう、当該プロバイダやサーバから前記ユーザやクライアントに送るデータにより当該ユーザやクライアントの機能を制御し、前記個人識別子毎に分けられるデータを当該プロバイダやサーバ内のファイルやメモリ等に蓄積してなる電子商取引システム不正検出方法の構成採用にある。

【００２５】本発明方法の第６の特徴は、上記本発明方法の第２、第３、第４又は第５の特徴における前記個人モデルと一般モデルが、統計処理を行うデータと状態遷移を表すデータの両方を含んでなる電子商取引システム不正検出方法の構成採用にある。

【００２６】本発明方法の第７の特徴は、上記本発明方法の第６の特徴における前記状態遷移が、アクセス行動から不正利用を検出する単独アクセス行動状態遷移と、過去から現在までの状態遷移の比較によって不正利用を検出する複数アクセス状態遷移とが存在してなる電子商取引システム不正利用検出方法の構成採用にある。

【００２７】本発明方法の第８の特徴は、電子商取引を行う任意のクライアント／サーバシステムに対する不正利用を検出するための電子商取引の不正利用を検出するに当り、クライアントからサーバに対しアクセスが開始された後、クライアントから所定のイベントが複数回にわたって発行されるごとに、サーバにおいて、クライアント及びそのユーザに関する情報並びに当該ユーザによる電子商取引行為に関する情報を複数のデータとして逐次取り込んで、当該複数のデータのそれぞれを、ユーザに付与される個人識別子を単位とした個人別モデルに組み込んで蓄積し、以後、新たにアクセスが実行されるごとに、当該アクセスが開始された後に得られる複数のデータと個人別モデルとを比較し、この比較結果に基づいて、当該アクセスが不正利用によるものであるか否かを判定してなる電子商取引システム不正利用検出方法の構成採用にある。

【００２８】本発明方法の第９の特徴は、上記本発明方法の第８の特徴における複数のデータの蓄積に際し、複数のデータのそれぞれを、個人別モデルに代え、当該システムを利用する全てのユーザの平均的データを得るための一般モデルに組み込んで行い、アクセスが不正利用

によるものであるか否かの判定は、複数のデータと当該一般モデルとを比較した結果に基づいて行ってなる電子商取引システム不正利用検出方法の構成採用にある。

【００２９】本発明方法の第１０の特徴は、上記本発明方法の第８又は第９の特徴における複数のデータの蓄積を、１回のアクセスが終了した時点で得られる全てのデータをその発生順に並べた時系列データによって行ってなる電子商取引システム不正利用検出方法の構成採用にある。

【００３０】本発明方法の第１１の特徴は、上記本発明方法の第１０の特徴における時系列データを得るに際し、所定のイベントが最後に発行されたと予想される時から所定の制限時間が経過した時点で、当該最後の所定のイベントまでを１回のアクセス中に含まれる一連の所定のイベントと見做してなる電子商取引システム不正利用検出方法の構成採用にある。

【００３１】本発明方法の第１２の特徴は、上記本発明方法の第８、第９、第１０又は第１１の特徴におけるアクセスが不正利用によるものであるか否かの判定を、統計学的手法を用いて行ってなる電子商取引システム不正利用検出方法の構成採用にある。

【００３２】本発明方法の第１３の特徴は、上記本発明方法の第８、第９、第１０、第１１又は第１２の特徴におけるアクセスが不正利用によるものであるか否かの判定を、１回のアクセス中に複数回にわたって発行される所定のイベントに伴う当該システムの状態遷移の不規則性を検出することにより行ってなる電子商取引システム不正利用検出方法の構成採用にある。

【００３３】本発明方法の第１４の特徴は、上記本発明方法の第８、第９、第１０、第１１又は第１２の特徴におけるアクセスが不正利用によるものであるか否かの判定を、複数のアクセスにおいて取り込まれる同一ユーザのものと予想される複数のデータのうち、特定のデータの不規則性を検出することにより行ってなる電子商取引システム不正利用検出方法の構成採用にある。

【００３４】本発明方法の第１５の特徴は、上記本発明方法の第１４の特徴における特定のデータが、ユーザによる電子商取引に関する情報から成るデータである電子商取引システム不正利用検出方法の構成採用にある。

【００３５】本発明方法の第１６の特徴は、上記本発明方法の第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における所定のイベントが、次の画面の表示を要求するための次画面表示要求イベントである電子商取引システム不正利用検出方法の構成採用にある。

【００３６】一方、本発明装置の第１の特徴は、電子商取引を行う任意のクライアント／サーバシステムにおけるサーバに、少なくとも、アクセスの開始と共にクライアントから送信されるアクセスデータを抽出するアクセスデータ抽出手段と、このアクセスデータ抽出手段により抽出されたアクセスデータを蓄積するデータ蓄積手段とを具備して成る電子商取引システム不正利用検出装置において、アクセスデータ抽出手段が、アクセスデータの抽出に加え、アクセスが開始された後、クライアントから所定のイベントが複数回にわたって発行されるごとに、クライアント及びそのユーザに関する情報並びに当該ユーザによる電子商取引行為に関する情報を包含する複数のデータを抽出する機能を持たせると共に、データ蓄積手段が、アクセスデータの蓄積に加え、アクセスデータ抽出手段により抽出された複数のデータのそれぞれを、ユーザに付与される個人識別子を単位とした個人別モデルに組み込んで蓄積する機能を持たせ、その上で、当該データ蓄積手段により蓄積された個人別モデルに組み込まれた複数のデータを、新たなアクセスが実行されるごとに、当該アクセスが不正利用によるものであるか否かを判定するための判定基準として供与する判定基準供与手段と、この判定基準供与手段により供与される個人別モデルに組み込まれた複数のデータと、当該アクセスに伴ってアクセスデータ抽出手段により抽出される新たな複数のデータとを比較して、当該アクセスが不正利用によるものであるか否かを判定する不正利用判定手段と、を備えてなる電子商取引システム不正利用検出装置の構成採用にある。

【００３７】本発明装置の第２の特徴は、上記本発明装置の第１の特徴におけるデータ蓄積手段が、複数のデータのそれぞれを、個人別モデルに代え、当該システムを利用する全てのユーザの平均的データを得るための一般モデルに組み込み、判定基準供与手段が、当該データ蓄積手段により蓄積された一般モデルに組み込まれた複数のデータを、新たなアクセスが実行されるごとに、当該アクセスが不正利用によるものであるか否かを判定するための判定基準として供与し、不正利用判定手段が、当該判定基準供与手段により供与される一般モデルに組み込まれた複数のデータと、当該アクセスに伴ってアクセスデータ抽出手段により抽出される新たな複数のデータとを比較して、当該アクセスが不正利用によるものであるか否かを判定する一連の有機的連係機能をそれぞれ持たせてなる電子商取引システム不正利用検出装置の構成採用にある。

【００３８】本発明装置の第３の特徴は、上記本発明装置の第１又は第２の特徴におけるデータ蓄積手段が、複数のデータの蓄積を、１回のアクセスが終了した時点で得られる全てのデータをその発生順に並べた時系列データによって行う機能を有してなる電子商取引システム不正利用検出装置の構成採用にある。

【００３９】本発明装置の第４の特徴は、上記本発明装置の第３の特徴におけるデータ蓄積手段が、時系列データを得るに際し、所定のイベントが最後に発行されたと予想される時から所定の制限時間が経過した時点で、当該最後の所定のイベントまでを１回のアクセス中に含ま

れる一連の所定のイベントと見做す機能を有してなる電子商取引システム不正利用検出装置の構成採用にある。

【００４０】本発明装置の第５の特徴は、上記本発明装置の第１、第２、第３又は第４の特徴における不正利用判定手段が、アクセスが不正利用によるものであるか否かの判定を、統計学的手法を用いて行う演算手段を有してなる電子商取引システム不正利用検出装置の構成採用にある。

【００４１】本発明装置の第６の特徴は、上記本発明装置の第１、第２、第３、第４又は第５の特徴における不正利用判定手段が、アクセスが不正利用によるものであるか否かの判定を、１回のアクセス中に複数回にわたって発行される所定のイベントに伴う当該システムの状態遷移の不規則性を検出することにより行う演算手段を有してなる電子商取引システム不正利用検出装置の構成採用にある。

【００４２】本発明装置の第７の特徴は、上記本発明装置の第１、第２、第３、第４又は第５の特徴における不正利用判定手段が、アクセスが不正利用によるものであるか否かの判定を、複数のアクセスにおいて取り込まれる同一ユーザのものと予想される複数のデータのうち、特定のデータの不規則性を検出することにより行う演算手段を有してなる電子商取引システム不正利用検出装置の構成採用にある。

【００４３】本発明装置の第８の特徴は、上記本発明装置の第７の特徴における特定のデータが、ユーザによる電子商取引に関する情報から成るデータである電子商取引システム不正利用検出装置の構成採用にある。

【００４４】本発明装置の第９の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７又は第８の特徴における所定のイベントが、次の画面の表示を要求するための次画面表示要求イベントである電子商取引システム不正利用検出装置の構成採用にある。

【００４５】

【発明の実施の形態】以下、添付図面を参照しつつ、本発明の実施の形態をその装置例及び方法例につき説明する。なお、以降の説明では、理解を容易なものとするため、クライアント／サーバシステムの例として、WWWを使ったインターネットのシステムを挙げてあるがユーザ／プロバイダシステムでも一向に構わない。

【００４６】（装置例）図１は、本発明の一実施形態に係る電子商取引システム不正利用検出装置の原理的構成を示すブロック図である。

【００４７】同図に示すように、この実施形態の係る電子商取引システム不正利用検出装置αは、まず、その前提として、電子商取引を行う任意のクライアント／サーバシステムにおけるサーバ（図示せず）に設置され、少なくとも、アクセスの開始と共にクライアント（図示せず）から送信されるアクセスデータを抽出するアクセスデータ抽出手段１と、このアクセスデータ抽出手段１により抽出されたアクセスデータを蓄積するデータ蓄積手段２とを具備して構成される。なお、データ蓄積手段２により蓄積されるアクセスデータは、実際には、ハードディスク等から成るアクセスデータ記憶手段３に記憶される。

【００４８】そして、この電子商取引システム不正利用検出装置αにおいては、上述のアクセスデータ抽出手段１が、以上のアクセスデータの抽出に加え、アクセスが開始された後、クライアントから、例えば、次の画面の表示を要求するためのイベント（次画面表示要求イベント）が複数回にわたって発行されるごとに、クライアントに関する情報並びに当該クライアントによる電子商取引行為に関する情報を包含する複数のデータを抽出するよう機能構成される。

【００４９】同時に、データ蓄積手段２が、アクセスデータ記憶手段３へのアクセスデータの蓄積に加え、アクセスデータ抽出手段１により抽出された複数のデータのそれぞれを、クライアントに付与される個人識別子を単位とした個人別モデルと、当該システムを利用する全てのクライアントの平均的データを得るための一般モデルに組み込んで蓄積するよう機能構成される。なお、データ蓄積手段２により蓄積される複数のデータは、その個人別モデル及び一般モデルにつき、ハードディスク等から成る個人別モデル記憶手段４及び一般モデル記憶手段５にそれぞれ記憶される。

【００５０】さらに、この電子商取引システム不正利用検出装置αは、データ蓄積手段２により個別モデル記憶手段４及び一般モデル記憶手段５に蓄積された個人別モデル及び一般モデルに組み込まれた複数のデータを、新たなアクセスが実行されるごとに、当該アクセスが不正利用によるものであるか否かを判定するための判定基準として供与する判定基準供与手段６と、この判定基準供与手段６により供与される個人別モデルに組み込まれた複数のデータと、当該アクセスに伴ってアクセスデータ抽出手段１により抽出される新たな複数のデータとを比較して、当該アクセスが不正利用によるものであるか否かを図示しない論理演算手段等を用いて判定する不正利用判定手段７とを有して構成される。

【００５１】ここで、データ蓄積手段２による複数のデータの蓄積は、１回のアクセスが終了した時点で得られる全てのデータをその発生順に並べた時系列データによって行うことも可能である。

【００５２】ただし、例えば、WWWサーバでは、アクセスが中断されたことを知るための手段が存在しないので、この時系列データを得る際には、イベントが最後に発行されたと予想される時から所定の制限時間が経過した時点で、当該最後のイベントまでを１回のアクセス中に含まれる一連のイベントと見做し、便宜的にクライアントの行動を連続化させる手法を採るとよい（所定の制限時間が経過した後は、一連のイベントとは見做さな

い）。

【００５３】また、不正利用判定手段７における、アクセスが不正利用によるものであるか否かの判定に際しては、演算手段等を駆使した一般の統計学的手法を用いて行い、さらに、特殊な手法として、１回のアクセス中に複数回にわたって発行されるイベントに伴う当該システムの状態遷移の不規則性を検出するようにしたり、或いは、複数のアクセスにおいて取り込まれる同一クライアントのものと予想される複数のデータのうち、例えば、クライアントによる電子商取引に関する情報から成る特定のデータの不規則性を検出するようにしてもよい（詳細は後述）。

【００５４】（方法例）次に、以上のように構成された装置例に適用する方法例を、その概要及び実施手順につき説明する。

【００５５】〔概要〕まず、WWWサーバにアクセスしてきているクライアントのサーバ内での行動を一連の行動として捉えるために、ＣＧＩ（Common Gateway Interface）やミドルウェアの設置によってWWWサーバ側で記録できるデータの種類を増やす。

【００５６】また、クライアントにはＩＤなどの個人識別子を持たせ、初期画面以降のページの移動時にその情報がサーバに自動的に送信されるよう、サーバからクライアントに送るデータによりクライアントの機能を制御し、個人識別子ごとに分けられるデータをサーバ内のファイルやメモリ（アクセスデータ記憶手段３）などに蓄積できるようにする。

【００５７】このデータによって、標準的なWWWサーバのログよりも多くの情報を記録でき、複数人物がほぼ同時刻にWWWサーバにアクセスしてきている状況であっても、特定の個人のWWWサーバ内での行動を抽出することができるようになる。

【００５８】ここで、正規クライアントと不正クライアントを識別するために利用されるのは、前述した個人別モデルと一般モデルの２種類のデータ群である。個人別モデルは、個人識別子ごとに、過去において当該WWWサーバで行われたクライアントの傾向や習性を表す行動履歴を保存しているデータの集合であり、一般モデルは、当該WWWサーバにおける全クライアントから求められる傾向や習性を表すデータの集合である。

【００５９】何れのモデルにおいても、単独のイベント記録から直接データが得られるものと、複数のイベント記録から導き出されるものの両方のデータを利用する。なお、複数のイベント記録とは、WWWサーバにアクセスを開始してからの個人識別子ごとに記録される一連の行動を集約化したものである。

【００６０】ここにおける個人別モデルと一般モデルは、統計処理を行うデータと状態遷移を表すデータの両方を含んでいる。統計処理を行うデータとは、数量化できるデータのことであり、数量化によって得られた傾向や習性を表す個人別モデル又は一般モデルと、現在アクセス中の個人識別子を持つ人物と違いを統計手法の検定などを用いて検証する。さらに、このデータは、１回のWWWサーバへのアクセス時だけから得られるデータと、複数回のWWWサーバへのアクセスから得られるデータの両方を含む。

【００６１】また、状態遷移にも２種類の検出方法を用い、その一方は、例えば、あるときのWWWサーバへのアクセス行動から、カタログを閲覧していない商品を購入しようとしている場合などといった不正利用とみなせる行動を検出するという単独アクセス状態遷移であり、他方は、例えば、過去３回の購入時に購入総額が上昇しつづけているクライアント、過去の購入金額の平均の５倍よりも大きな額を購入しようとしているクライアントなどといった過去から現在までの状態遷移の比較によって不正クライアントを検出する複数アクセス状態遷移である。

【００６２】何れの場合も、不正クライアントと見做す基準となるルールをあらかじめ登録しておき、ルールに該当する場合に不正クライアントと見做す。ただし、このルールは、クライアントのアクセスが増えるたびに累計演算し直して改定するため、固定的な値を持つものとはならない。

【００６３】〔実施手順〕まず、アクセスデータ抽出手段１において、クライアントが個人識別子を用いてWWWサーバにアクセスを開始したことが検出されると、データ蓄積手段２は、アクセスデータ記憶手段３に対し、その個人識別子に関するアクセスデータの記録を開始する。この時点において、接続元の情報として、クライアントのＩＰアドレス（ＩＰ： Internet Protocol）、ブラウザの種類などが得られるため、これらの情報を、アクセスが不正利用によるものであるか否かを検出する際の正規クライアントと不正クライアントの識別のための一情報として用いる。

【００６４】次に、この後にクライアントがサーバ内で行うページの移動に関する行動、即ち次画面表示要求イベントを、アクセスデータ抽出手段１及びデータ蓄積手段２を用いて、個人別モデル記憶手段４及び一般モデル記憶手段５に逐一記録することにより、当該クライアントがWWWサーバにアクセスした瞬間から、これを時系列データとして取り扱うことができるようにする。

【００６５】以上の状態において、アクセスデータ抽出手段１において新たなアクセスが検出され、このときのアクセスが不正利用によるものであるか否かを判定しようとする場合、判定基準供与手段６は、個人別モデル記憶手段４及び一般モデル記憶手段５に記憶された対応する個人別モデル及び一般モデルを読み出して、これを判定基準として不正利用判定手段７に供与する。

【００６６】そして、この不正利用判定手段７において、その供与された個人別モデル及び一般モデルを用い

て（又は選択的に用いて）、統計処理と状態遷移のルールとの比較により、アクセスが不正利用によるものであるか否かを判定し、これを不正利用判定結果としてサーバのプロセッサ（図示せず）に転送する。なお、ここで不正クライアントを検出するための基準は、電子商取引システムの目的、取り扱う商品の内容、WWWのページ構成などによって変化するため、固定的な基準にはならない。

【００６７】なお、電子商取引システムにおいては、前述もしたように、所要の不正利用の検出をリアルタイムで行う必要があり、しかも、その検出は通常、複数のデータを用いて行われるため、その際のデータ解析が、サーバ処理に負荷をかけてしまう結果となる。

【００６８】このための方策としては、例えば、個人別モデル及び一般モデルにおける各々のデータに対し、実際の判定に用いる際の優先順位を与えておき、その順位が高いデータから不正利用の検出に利用するようにし、これにより、できるだけ少ないデータの検証で不正クライアントの検出ができるようにして、サーバへの負荷を減らすようにするとよい。

【００６９】また、アクセスが不正利用によるものであるか否かを判定すべき状況においても、それが不正利用であるか否かによらず、クライアントのアクセス状態を表すデータについては一様に保存し、これをクライアントのアクセス履歴情報として蓄積するようにする。このとき、必要があれば、統計処理時に不正利用とみなすための基準と状態遷移ルールに、クライアントアクセスの状態を反映させるようにするとよい。

【００７０】

【実施例】最後に、実施例として、以上に説明した装置例及び方法例の実際の電子商取引システムへの応用につき説明する。

【００７１】（第１実施例）

○物品販売を行う電子商取引システムの事例

この例は、インターネット上のWWWサーバで商品カタログを提示し、クライアントがそれらの商品を選択、購入し、必要な場合には決済もできるものである。この場合、商品の閲覧だけでは金銭的な被害は発生しないため、決済が行われる前に不正利用を検出すれば良い。

【００７２】従って、クライアントがサーバにアクセスを開始した時点から決済を行う直前までに集めた多くのデータを用いて、不正クライアントの検出を行うことができ、不正クライアントの検出の誤りを少なくすることができる。なお、ここでの検出の誤りとは、正規クライアントのアクセスを不正クライアントのアクセスと見做してしまうことと、不正クライアントのアクセスを正規クライアントのアクセスと見做してしまうことの両方が含まれる。

【００７３】（第２実施例）

○会員に情報を提供する電子商取引システムの事例

この例は、あらかじめ登録されたクライアントだけに情報を提供する電子商取引システムである。この例と先の物品販売を行う電子商取引サーバの事例との違いは、決済するまでに不正利用を検出すれば良いのではなく、クライアントが情報を閲覧し始めた時点から出来るだけ早く不正利用を検出して、これを排除する必要があるということである。

【００７４】その理由は、この種の電子商取引システムの場合は、提供される情報自体に価値があるため、情報の漏洩という被害を少なくするために不正利用の早期検出が不可欠であること、また、情報にアクセスするたびに決済が行われるわけではないので、決済の期間が長いということなどが挙げられる。

【００７５】なお、本例の場合、物品販売を行う電子商取引システムの事例と違い、物品販売による金銭の授受が無いため、WWWサーバ内でのクライアントの行動データだけから不正クライアントを識別する必要があるが、装置の基本構成については何ら変わりはない。あくまで、不正クライアントの判定データと基準が異なるだけである。

【００７６】以上、本発明の実施の形態並びに第１及び第２の実施例につき、クライアント／サーバシステムの例として、WWWを使ったインターネットのシステムを挙げて説明したが、無論、本発明は、電子商取引を行うことの可能な任意の形態を成すクライアント／サーバシステム及びユーザ／プロバイダシステム全般につき適用しうるものである。また、本発明は、必ずしも上述した手段及び手法にのみ限定されるものではなく、本発明にいう目的を達成し、後述する効果を有する範囲内において、適宜、変更実施することが可能なものである。

【００７７】

【発明の効果】以上説明したように、本発明によれば、クライアントからサーバに対しアクセスが開始された後に発行される種々の複数のデータを取り込み、これら一旦取り込んでおいた複数のデータのそれぞれと、以後、新たにアクセスが実行されるごとに当該アクセス後に得られる複数のデータとを比較し、この比較結果に基づいて、当該アクセスが不正利用によるものであるか否かを判定するようにした。

【００７８】それ故、正規ユーザや正規クライアントの通常の行動を監視した結果に基づいて不正ユーザや不正クライアントによるシステムの不正利用を検出することが可能になると共に、同一ユーザやクライアントにより為された一連の行動を把握することが可能となり、さらに、一般的なユーザやクライアントの行動様式に基づいてシステムの不正利用を検出することも可能となる。この結果、物品販売などを行う電子商取引システムの運用者に金銭的な被害などの及ぶ可能性が非常に低くなる。

【図面の簡単な説明】

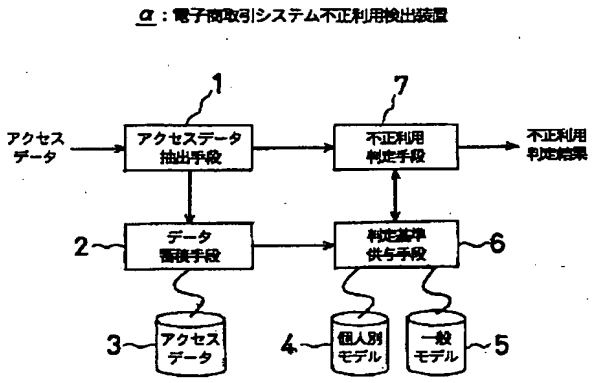
【図１】本発明の実施形態に関わる不正利用検出装置の

構成を示すブロック図である。

【符号の説明】

α…電子商取引システム不正利用検出装置
１…アクセスデータ抽出手段
２…データ蓄積手段
＊３…アクセスデータ記憶手段
４…個人別モデル記憶手段
５…一般モデル記憶手段
６…判定基準供与手段
＊７…不正利用判定手段

【図１】



This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.